

U.S. TREASURY CHIEF INFORMATION OFFICER TESTIMONY

BEFORE THE

HOUSE SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

Mr. Chairman and members of the Subcommittee, thank you for the opportunity to appear to discuss the state of Treasury's information technology (IT) security and financial reporting, as well as the actions underway for remediating the material weaknesses. The continued leadership of the Chairman and the members of the Subcommittee is critical if we are to improve IT security and accountability not only at Treasury but across the federal government.

I serve as the Chief Information Officer (CIO) of the Treasury Department. As CIO I provide oversight, strategic management, and policy direction of all information technology security programs within the Treasury Department and its Bureaus. In addition, I have operational responsibility for shared Enterprise services across all

Treasury bureaus, including the cyber protection measures applied to these services.

As articulated by the recent OMB report to the Congress on Federal Government Information Security Reform, IT security is a continuing challenge that warrants the attention of the Congress, the Executive Branch, industry, academia, and the taxpayer–citizens whom we serve. It is vital to our nation’s financial institutions, economic prosperity, homeland defense, and E–Government service efforts. It is also crucial to achieving the Treasury’s strategic objectives, and the Department continues to make great progress in improving the security of its IT systems. The Department has taken a number of measures to improve the overall IT security posture of the Department and to rectify the identified deficiencies in our GISRA FY 2002 submission to the Office of Management and Budget (OMB).

The present state of Treasury’s IT security requires improvement to achieve our objective of closing all IT–related material weaknesses as identified by the Government Information Security Reform Act (GISRA) FY 2002 review process. As of March 31, 2003, the Department had

14 material weaknesses. These included nine (9) at the Internal Revenue Service (IRS), three (3) at Financial Management Service (FMS), one (1) at the Mint, and one (1) at Departmental Offices (DO).

These weaknesses can be divided into two main categories:

information technology (IT) security weaknesses and financial management weaknesses, with additional general weaknesses at the IRS. First I will address IT security issues, and then I will cover financial reporting.

Central to the IT security material weaknesses is that the Department has not yet achieved the goal of full certification and accreditation (C&A) of mission critical systems and major applications. In addition, specialized IT security training and incorporation of security into the capital investment planning process need improvement. Also included in the list of deficiencies are new and repeated material weaknesses identified by the General Accounting Office (GAO).

To bolster IT security, Treasury has undertaken a number of actions to date to resolve outstanding issues addressed by the

Treasury Inspector General (IG) and Treasury Inspector General for Tax Administration (TIGTA). First, Treasury has implemented an aggressive oversight and compliance program for IT security. Program reviews of each Bureau are conducted to evaluate progress in six areas: 1) security policy and guidance; 2) computer incident handling and response capability; 3) security training; 4) Plan of Actions and Milestones (POA&M) management; 5) integration of security into capital planning; and 6) system C&A. During FY 2003 reviews will have been completed of all Bureaus' IT security programs to establish a baseline for future annual reviews. This is the first time the Department has conducted a complete review of its security programs. Treasury now requires all Bureaus to use the National Institute of Standards and Technology (NIST) Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," for performing self-assessments of both their IT security programs and general support systems and major applications. In addition Treasury has developed and is using a security oversight

methodology and checklist based on NIST 800–26 for conducting department–wide security reviews.

Second, to maximize implementation success and accountability, Treasury has set specific goals to improve security with the use of performance measures. For example, 80% of all Treasury systems must be certified and accredited by the end of FY 2003. This target has been conveyed to the Bureau Heads by the Secretary and to their CIOs by the Assistant Secretary for Management and Chief Financial Officer. Progress of each Bureau is being tracked on a quarterly basis as we move towards reaching the Treasury C&A goal. Our C&A performance measure goal for FY 2004 is 90%.

Third, a combined Federal Information Security Management Act (FISMA) 2003 data call has just been instituted by the Treasury CIO, IG and TIGTA. This joint data call is expected to remedy the inconsistency in reported numbers from the last two surveys performed under GISRA. An enterprise corrective Action Plan and Milestone process for tracking and mitigating each Bureau’s material weaknesses and deficiencies has been developed and implemented.

At present this is a manual process but plans are underway – as a cornerstone of Treasury’s IT governance reform – to provide an enterprise portfolio management capability by which the Department and all Bureaus will have online access for tracking and will be able to update their status in meeting the established milestones.

Fourth, Treasury has taken further action to ensure the protection of our critical infrastructure cyber assets. We have established a Critical Infrastructure Protection (CIP) Working group consisting of representatives from all its Bureaus. A Project Matrix review to identify key Treasury critical assets is being conducted and a Treasury-wide CIP policy and a Critical Infrastructure Protection (Strategic) Plan with an associated Treasury CIP Implementation Plan have been developed and issued. Treasury has completed and issued to its Bureaus an Interdependency Analysis Guideline/Methodology for completing the next step of the Project Matrix. Treasury is in the process of prioritizing our critical cyber assets and conducting interdependency analyses on those identified as supporting national critical functions and services.

Fifth, to augment the FISMA requirement for periodic security training, Treasury has scheduled an IT security conference for the Bureaus' IT security managers and staffs. The conference will include high-level training sessions and some targeted technical sessions focused on Treasury IT security issues. Additional C&A training is planned for Treasury's senior officials who are Designated Accrediting Authorities (DAA) for IT general support systems and major applications. To share training and awareness information and tools across all Bureaus, the Department has established an IT Security Training Forum which meets quarterly.

The Department is concerned about the new and repeat material weaknesses that have surfaced and continue to remain on the books. Consequently, Treasury is committed to identifying the root causes of unacceptable IT security and putting in place the structures, processes, and systems that will ensure the Department has a strong security regime. Let me describe several key initiatives that I consider essential to our reform.

First, as soon as I began as Treasury CIO, I decided that my number one priority as Treasury CIO would be IT governance. In short, pursuant to the Clinger–Cohen Act, the CIO’s mission is to ensure that the Department wisely stewards the funds of our taxpayer–citizens on technology and systems so that we can deliver valuable E–Government and other services. Establishing the right structures, processes, and systems of sound IT governance not only provides for sound planning and budget allocation but also necessitates incorporating security considerations into our capital planning and investment controls. It is a cardinal rule in business operations that the quality of a design has a disproportionate impact on the lifecycle cost of a system; if Treasury’s systems are not secure when we develop and deploy, the Department leaves itself vulnerable until deficiencies are remediated, and taxpayer dollars are not stewarded. An additional benefit is that, as Treasury increasingly aligns its IT operations with Department goals and objectives across the Department, achieving a more integrated, cohesive, and institutionalized security regime across Treasury is facilitated. In

short, achieving a strategic, robust, and integrated security regime across the Department will be severely limited if our capital planning and investment control process does not share those same characteristics.

Therefore, Treasury seeks to integrate its security programs both functionally with our capital planning process and organizationally across Bureaus. In addition to the security oversight provided by the Office of the CIO, the Bureaus are required by policy to establish complementary capabilities within their respective bureaus to perform annual self-assessments of their security postures. To ensure that security is consistently implemented across the Department, a set of comprehensive IT security policies, standards and procedures have been developed and issued to all Bureaus. These policies address state-of-the-art technologies and capabilities and provide management, operational and technical controls. A recently established Treasury IT Security Policy Forum meets quarterly to discuss proposed policies and standards which are binding on all Bureaus.

Second, in addition to implementing a new IT governance regime, the Department is working on an enterprise architecture that incorporates a strict IT security regime. This will represent a baseline by providing the security for integration into the performance, business and technical reference models in accordance with OMB's Federal Enterprise Architecture framework. The Bureaus' security architecture will be based on these security models and will provide consistency and interoperability across all platforms and applications where needed. Given Treasury's role in managing Federal Finances and collecting taxes and debts, as well as its role in investigating, tracking and reporting terrorist funding, money laundering, and other financial crimes, it is imperative that data transmissions are secure and private. Without the structure to protect the systems on which information relies, Treasury's ability to carry out its mission will be severely impacted. Owing in no small part to the enterprise architecture effort, the Department is making genuine progress in assuring these objectives are realized.

Third, proactive interagency collaboration on IT security provides additional evidence of the institutionalization of Treasury's IT security. Let me provide a few examples:

- The Treasury Communications System, the Department's nationwide business enabling communications networking infrastructure, is the largest secure and encrypted network in the civilian federal government. It routinely handles over 900 gigabytes of data securely each day and was the model used to establish the initial secure networking capabilities (Customs and Border Protection and Secret Service) of the newly formed Department of Homeland Security. The cyber security protection mechanisms applied to the Treasury Communications System were significantly enhanced in FY 2002. Additionally, a "security in depth" posture was deployed that resulted in a ten fold strengthening of the cyber security countermeasures of these communications services. This centrally managed capability is correlated to the Department of Homeland Security Threat Warning Level system. Any increase in threat level above

yellow results in continuous (24 hours per day) staffing to immediately respond to cyber initiated attacks.

- The Department is one of four agencies (Treasury, Department of Defense, Department of Agriculture, and NASA) to be cross-certified with the Federal Public Key Infrastructure (PKI) Bridge. Therefore, Treasury is positioned to strengthen its secure communications processes in conjunction and in alignment with its development of a common infrastructure.
- Although the missions of the Treasury Bureaus may be diverse, each Bureau is faced with the same challenges of physical, logical and cyber security, the need to improve business processes, the goal to be more resource conscious and the requirement to implement e-government initiatives. The Department determined smart cards and related security technologies, including leveraging its Public Key Infrastructure (PKI) cross-certification with the Federal PKI Bridge and biometrics, would provide the means to authenticate employee identification; secure facilities, systems, and property; and simplify a number of internal business processes.

Treasury, among other selected agencies (e.g., Department of Defense, Transportation Security Administration), is currently deploying smart cards with these technologies enabled at a number of its bureaus, including Departmental Offices.

- As cited previously, the Office of the CIO established a computer security incident response capability to coordinate Treasury efforts with appropriate external Computer Emergency Response Teams and to collect agency-wide information and to disseminate relevant incident reports within Treasury. This security response capability is coordinated with a similar government-wide effort managed through the Federal CIO Council.
- Treasury was recently recognized by the National Communications System (NCS) for enabling a thousand fold increase in circuits designated with the Telecommunications Service Priority (TSP) capability, thereby enhancing its ability to ensure reliable telecommunications during emergency situations – including on September 11, 2001.

- The Treasury CIO is the chairperson for the e-Authentication Steering Committee, the crosscutting government group working to ensure secure financial transactions and communications across the federal government.
- The Financial Management Service bureau continues to provide and expand its robust, reliable, redundant and secure technology infrastructure that issues payments for Social Security Benefits, Tax Refunds, Office of Personnel Management (OPM) Salary, Veterans Administration (VA) Retirement, Railroad Retirement Benefits, and many other forms of payment to the taxpaying public (approximately 900 million payments valued at approximately \$1.9 trillion with 99.999% reliability).
- The Department of the Treasury and the entire Finance and Banking Information Infrastructure Committee (FBIIIC) have been galvanized and positioned to harness and channel divergent security activities for that entire sector's benefit. To ensure the privacy of any electronic communications associated with the

augmentation of the sector's security improvements, Treasury implemented, and National Security Agency (NSA) approved, secure communications infrastructure specifically designed to support the activities of the FBIIC.

With respect to financial management material weaknesses, Treasury is overseeing remediation at two bureaus: the Internal Revenue Service and the Financial Management Service. Weaknesses at the IRS deal with property management, revenue reporting and financial statement preparation. Weaknesses at the Financial Management Service involve consolidated financial statements and check reconciliation.

The three weaknesses tied to financial reporting for the IRS are not scheduled to be closed this year but are covered in the IRS' Federal Financial Management Improvement Act Remediation Plan that Treasury provides to the Office of Management and Budget on a quarterly basis. In order to address the property management weakness, IRS will acquire and install a fixed asset module to the Integrated Financial System (IFS) that will generate records and record

capital asset acquisition costs in the appropriate general ledger. In the interim, IRS is interfacing the Information Technology Asset Management System (ITAMS) with IFS.

In order to provide support data for the revenue collected for employment and excise taxes, IRS is developing the Custodial Accounting Project (CAP). CAP will be a single, integrated data repository of taxpayer account information, integrated with the general ledger and accessible for management analysis and reporting. IRS intends to correct the lack of accurate general ledger account balances related to financial statement preparation by developing, documenting, and implementing new policies and procedures for monthly reconciliation and developing other steps.

The Consolidated Financial Statement weakness for the Financial Management Service is expected to be carried into 2004. FMS has undertaken a series of steps to improve revenue and net cost reconciliation procedures through implementation of Treasury, Office of Management and Budget, and General Accounting Office task force recommendations for the consolidation process. In the area of check

reconciliation, FMS is undertaking reconciliation as far back as records are reasonably available to investigate the cause of the imbalance and develop and to implement procedures for monthly reconciliation.

In the Office of the CIO, our mission is to “Steward Treasury’s information resources with integrity and professionalism.” That imperative is what the Clinger–Cohen Act and other statutes require, and it’s what our taxpayer–citizens expect. I remain committed to doing that, which requires developing a strong and dynamic IT security program, continuing to work to fulfill our statutory responsibilities in protecting sensitive and classified systems, leading the Bureaus in security policy and standards development, and raising IT security awareness across Treasury. Any weaknesses that threaten to impede our Department’s ability to achieve its mission we have aggressively sought to identify, analyze, and aggressively remediate, and we will continue to do so.

Again, I am grateful to the subcommittee for demonstrating leadership in identifying IT security as an issue and for driving reform

across the Federal Government. Mr. Chairman, thank you for the opportunity to appear before you today. This concludes my formal remarks, and I would be happy to respond to any questions.